

NCDOT Technical Architecture Specifications

The following Appendix delineates the NCDOT Technical Architecture Specifications for this RFP. These specifications are NCDOT's current Architecture standards based on the North Carolina Statewide Technical Architecture (NCSTA) found at <https://it.nc.gov/services/it-architecture/statewide-architecture-framework> and the North Carolina Statewide Information Security Manual found at: <http://it.nc.gov/statewide-resources/policies>.

All respondents shall explain and include specifications and technical literature sufficient to allow the Agency to determine that equipment and proposed technical solutions comply with these requirements and meet the project objectives. If a requirement is not addressed in the technical literature, it must be supported by additional documentation included with the response.

Technical details, including architectural diagrams with supporting narrative, shall be provided to NCDOT for assessing the adequacy of the proposed solution in meeting architecture and security requirements. High level marketing brochures will not provide sufficient detail.

A. Logical Application Environment

As detailed in the NCSTA, there must be clear separation between the presentation, business logic, and data components of the solution that are typically deployed on different physical/virtual machines.

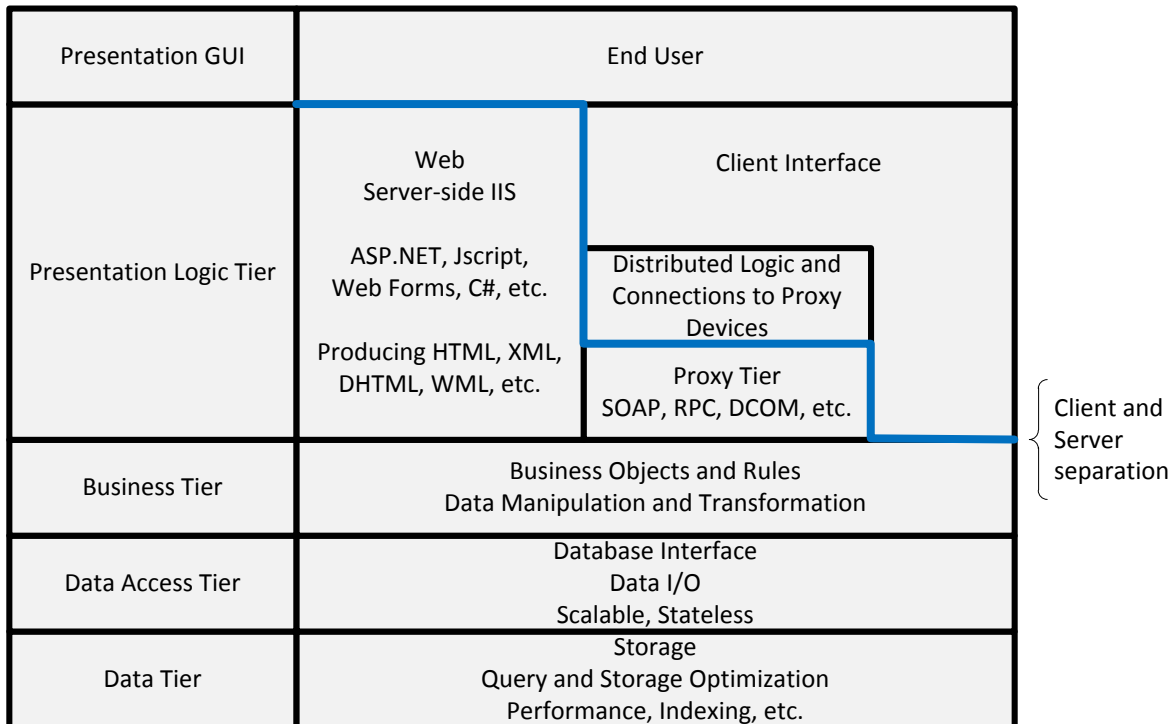


Figure 1. Logical Environment

B. Logical Network Environment

All environments of the proposed solution shall function within the network topology described below.

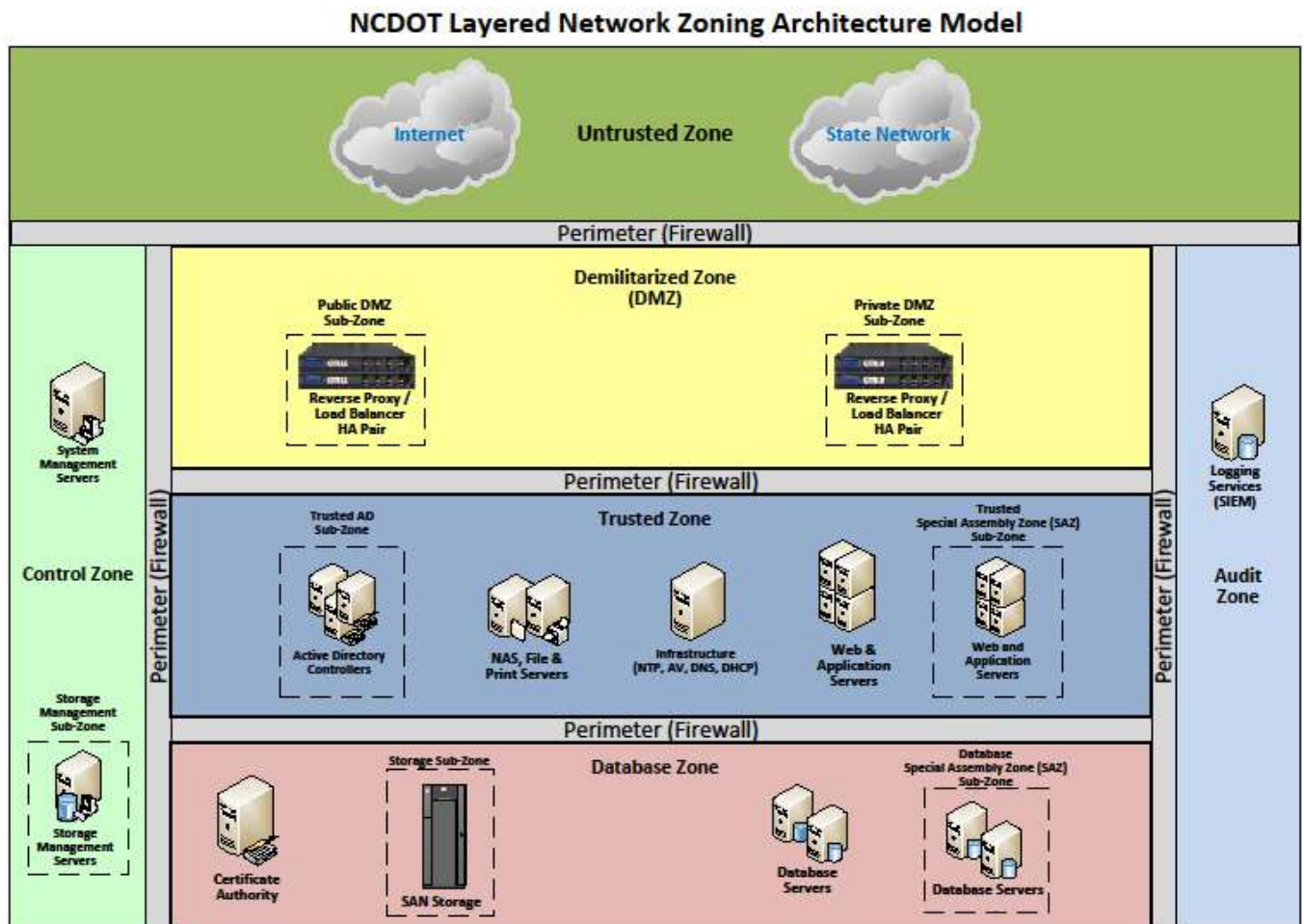


Figure 2. NCDOT Layered Network Zoning Model

1. Untrusted Zone

Untrusted zones comprise systems and networks unknown to the Agency or known to be a serious security risk. Access to and from untrusted zones is normally limited to DMZ systems, and untrusted zones do not have direct access to higher trust zones. Access to higher trust zones from untrusted zones must be through an intermediate trusted system.

Examples: Internet, business partners, other State agencies

2. Demilitarized Zone (DMZ)

DMZs are comprised of systems controlled by NCDOT, but that are exposed to untrusted systems. These zones are the gateway to more trusted and restricted zones. These systems pose a risk to the organization due to the potential for direct compromise and their critical role as portals to internal systems and application servers as well as internal networking resources. DMZs can be further delineated to serve specific security zoning based on client type such as internal DMZ, external DMZ, partner DMZ, etc.

Examples: Public facing web servers (external sub-zone), internal facing web servers (internal sub-zone), remote access devices (remote access sub-zone), and public facing DNS (DNS sub-zone).

3. Trusted Zone

The trusted zone is comprised of systems owned and controlled by NCDOT, and may also include trusted systems owned and operated by trusted outside entities. This zone is where most day-to-day business activities with low individual and high aggregate value take place. Enterprise controlled systems in this zone are configuration controlled to ensure that appropriate technical controls are in place. The trusted zone does not have direct adjacency to untrusted zones, and is buffered by DMZ zoning. The trusted zone therefore does not support direct connectivity from untrusted zones, but could support connections from the trusted zone outbound to untrusted zones in some cases.

Examples: NCDOT client computers, web and application servers

4. Database Zone

The database zone encompass systems owned, controlled by, and known to NCDOT, but that represent a significant security risk and require additional access restrictions. Systems in the data zone will have very conservative and specific security policies applied, only allowing communication between prescribed systems and only between trusted zones. Systems in the database zone require higher levels of configuration and change control are only open to connections from a limited number of other carefully controlled systems.

Examples: Data Storage, Database services, Certificate Authority

5. Control Zone

The control zone performs separation of network, security, and host management from normal business transaction zones. This zone provides a single highly trusted and secure zone for the Agency to manage infrastructure. The control zone has unfettered access to all zones in order to manage all infrastructure in each zone. Although the control zone has access to all other zones, policies are employed to limit access to required services necessary to manage infrastructure.

Control zones may be sequestered similarly to business function zones via dedicated VLANs and perimeters such as firewall interfaces and policy. Control zones may also be networks isolated from outside and client networks altogether or supported logically via encryption between management hosts and managed hosts.

6. Audit Zone

The audit zone is a dedicated zone for receiving and storing system audit information such as syslog, SMTP traps, and other alerts and forensic data. The audit zone is configured to only receive traffic from all other zones. All processing and reporting on audit information is normally handled within the audit zone itself. As the audit zone performs a forensic function, access to the zone by systems and personnel is highly managed. This model allows the audit zone to maintain data confidentiality and integrity. Like the control zone, the audit zone can be isolated by network configuration or even supported logically via encryption.

7. Subzones

Subzones are a special class of zoning where a service shares the majority of business functions and/or security requirements of other services within a given zone, but also has a significantly more restrictive security or business requirement that would limit interaction of the service with its zone peers.

Subzones exist logically within existing zones but have their own security policy perimeter. A given zone could have multiple subzones, but similar to the management of the parent zones a balance between the number of subzones and clear requirements should be struck. It is feasible for a subzone to be further subdivided.

An example of a subzone may include a service located within the DMZ zone that has similar inbound and outbound policy as applied to untrusted zone clients but is limited or disallowed from interacting with peers within the DMZ zone itself.

8. Perimeters

Zone perimeters are logical and sometimes physical boundary between zones where security policy is defined and enforced. Perimeters may be as simple as VLANs and network layer-3 segmentation, or as complex as defined firewall rules, intrusion prevention system monitoring, VPN, proxy access or other security solutions.

In a layered architecture, inner zones with higher trust will often build upon previous zones' policies to add more granular security in zone progression.

C. Interfaces

All web services interfaces shall be compliant with the Web Services Interoperability standard. Where possible, XML schemas shall be derived from industry standard vocabularies, such as the National Information Exchange Model (NIEM).

All interfaces shall include validation processes to ensure the completeness and integrity of all transmitted or received data.

D. Server Virtualization

If the proposed solution is a NCDOT hosted "on premise" solution NCDOT desires to host the proposed solution in a VMware vSphere virtualized environment. Respondents shall state whether the proposed solution operates in a virtualized environment and shall provide details of any limitations or special requirements for operating in a virtualized environment.

E. Hardware and Software Specifications

The following tables represent NCDOT's current hardware and software standards. Whenever a material, article or piece of equipment is identified in this specification(s) by reference to a manufacturer's or Vendor's name, trade name, catalog number or similar identifier, it is intended to establish a standard, unless otherwise specifically stated as a brand specific requirement (no substitute items will be allowed).

1. End User Software:

The following table represents NCDOT's current End User software standards and is provided to give vendors an understanding of End User computing capabilities.

Component	Standard
Operating System	Windows 7 Enterprise Currently planning migration to Windows 10
Word Processor	Microsoft Word 2013 as part of Office365
Spreadsheets	Microsoft Excel 2013 as part of Office365
Presentations	Microsoft PowerPoint 2013 as part of Office365
E-Mail Client	Microsoft Outlook 2013 as part of Office365
Project Management	SAP Project Systems Microsoft Project 2013
Graphics – Flowcharting/Diagramming	Microsoft Visio 2013
Web Browser	Microsoft Internet Explorer 11

Component	Standard
PDF Viewer	Adobe Reader 11
PDF Writer	deskPDF Creator
Antivirus and Host-Intrusion Detection	McAfee VirusScan Enterprise
File Integrity Monitoring (FIM)	McAfee Change Control FIM File Integrity Monitoring shall be installed on all applicable devices considered Highly Restricted according to NCDOT's Data Classification Policy
Patch Management	Microsoft System Configuration Manager (SCCM) Microsoft Windows Server Update Services (WSUS)
Mainframe Terminal Emulation	IBM Personal Communications
Thin Client Access	Citrix Receiver Client
Instant Messaging	Microsoft Skype for Business
Web Conferencing	Microsoft Skype for Business
Full Disk Encryption	McAfee Endpoint Encryption Full Disk Encryption shall be installed on all applicable devices considered Highly Restricted according to NCDOT's Data Classification Policy
Remote Support Tool	Bomgar
CADD	Bentley MicroStation, Geopak and Iplot
Logging Agent	IBM QRadar WinCollect agent

2. End User Hardware:

The following table represents NCDOT's current End User hardware specifications and is provided to give vendors an understanding of End User computing capabilities.

Component	Minimum Desktop Specifications (in current use)	New Desktop Specifications	Minimum Laptop Specifications (in current use)	New Laptop Specifications
CPU	AMD Phenom II X4 (3.0GHz, 6MB cache)	Intel Core i5-4590 Quad Core (3.3GHz, 6MB cache)	Intel Core i5-430M (2.26GHz, 3MB cache)	Intel Core i5-4340M Dual Core (2.9GHz, 3M cache)
Hard Disk	160 GB SATA HD	500 GB SATA HD	160 GB SATA HD	500 GB SATA HD
Memory	4.0 GB	8.0 GB	4.0 GB	8.0 GB
Monitor	19" TFT (1280x1024)	20" TFT (1440x900)	14" WXGA TFT (1366x768)	14" WXGA TFT (1366x768)
Video Card	Integrated graphics / ATI Radeon HD 4200	AMD Radeon R5 240 w/ dual monitor support	Integrated Intel HD Graphics 3000	Integrated Intel HD Graphics 4600 w/ dual monitor support

Component	Minimum Desktop Specifications (in current use)	New Desktop Specifications	Minimum Laptop Specifications (in current use)	New Laptop Specifications
Operating System	Windows 7 Enterprise, 32 & 64 bit	Windows 7 Enterprise, 32 & 64 bit	Windows 7 Enterprise, 32 & 64 bit	Windows 7 Enterprise, 32 & 64 bit

3. Wireless Data Connectivity:

The following table represents NCDOT's current End User wireless standards and is provided to give vendors an understanding of End User capabilities.

Component	Environment
Wireless Data Connectivity	Verizon Wireless Cellular data 3G, 4G LTE Wi-Fi (WPA2 Enterprise Security)

4. General Server Standards:

Servers needs are determined based on many factors, including utilization of existing Infrastructure, requirements of planned projects, and the availability of specific funding for new equipment. Some platforms will share components and others will not, depending upon the unique circumstances for each project and product. Sharing and re-use are promoted when feasible. NCDOT's goal is to provide a homogeneous environment to streamline support and maximize resources, using virtual environment and consolidated server farms supporting many applications.

Component	Standard
Operating System	Microsoft Windows Server 2012 R2
System Virtualization	VMware vSphere v6.1
Processor Type	Intel Xeon
Backup	NetApp SnapProtect NetApp SnapManager for VI NetApp SnapMirror Commvault Simpana (physical servers only)
Storage	NetApp FAS Storage Systems
E-Mail	Microsoft Exchange Online as part of Office365
Web Server	Microsoft Internet Information Server – IIS 8.5
Application Server	Microsoft .NET Framework 4.6.1
Antivirus and Host-Intrusion Detection	McAfee VirusScan Enterprise
File Integrity Monitoring	McAfee Change Control FIM File Integrity Monitoring shall be installed on all applicable devices considered Highly Restricted according to NCDOT's Data Classification Policy
Server Patching	Microsoft System Center Configuration Manager (SCCM) Microsoft Windows Server Update Services (WSUS)
System Logging	IBM QRadar WinCollect agent

5. Application Development:

The following table represents NCDOT's current Application Development standards.

Component	Standard
Database Software	Microsoft SQL Server 2012 SP2
Application Development Frameworks	.NET Framework v4.61
Application Virtualization	Citrix XenApp Microsoft AppV
Software and Development Tools	Microsoft Visual Studio 2015
GIS	ESRI ArcGIS Platform v10.3
Version Control, Release, Defect , Deployment and Issue Management	Microsoft Team Foundation Server (TFS) 2015
LDAP/Directory/Authentication	Microsoft Active Directory Optimal IdM – Virtual Identity Server (VIS) NCID – North Carolina Identity Management
Single Sign On	SAML v2.0 WS Federation 1.1
Middleware	Web Services (SOA) Microsoft BizTalk 2013 (ESB)
Web Service - Data Formats	XML EDI XSLT
Web Service – Data Exchange	National Information Exchange Model (NIEM) SOAP REST
Web Service – Service Description Interface	WSDL
Software Testing (Functional, Performance, & Load)	HP Quality Center, HP Performance Center

6. Enterprise Solution Platforms:

The following table represents NCDOT's current Enterprise Solution Platform standards.

Platform	Standard
Enterprise Reporting	Microsoft SQL Server Reporting Services
Enterprise Resource Planning (ERP)	SAP ECC
Business Intelligence	SAP Business Warehouse SAP Business Objects Suite
Enterprise Content Management	Microsoft SharePoint 2013 Enterprise
Document Scanning/Imaging	EMC Captiva InputAccel

Platform	Standard
eForms and Digital Signatures	DocuSign
Web Search Engine	Microsoft SharePoint 2013 Enterprise Search
Reverse Proxy & Load Balancing	Citrix NetScaler appliances
Voice Communications	Avaya VoIP
Address Verification	Experian QAS Web Pro
Service Desk	FrontRange Heat
Enterprise Change Management	Open-source Ticketing Request System (OTRS)
System and Application Updating and Patching	Microsoft System Configuration Manager (SCCM) Microsoft Windows Server Update Services (WSUS)
Security Information and Event Management (SIEM)	IBM QRadar SIEM

F. Software Development Life Cycle

To support the NCDOT Software Development Life Cycle (SDLC), the proposed solution shall provide for at least but not limited to System Integration and User Acceptance Testing.

G. Networking Requirements

If the proposed solution is a NCDOT hosted “on premise” solution NCDOT shall be responsible for all network components required to provide the application access to the NCDOT network.

For all proposals the vendor shall define all networking requirements of the proposed solution including but not limited to:

- Minimum network bandwidth requirements, expressed in kilobits per second (kbps) or megabits per second (Mbps) for all proposed solution components.
- Minimum network latency requirements, expressed in milliseconds (ms) for all proposed solution components.
- Network availability requirements for all proposed solution components.

H. Authentication and Authorization

The proposed solution shall use role-based access control and security. It is preferred that the user provisioning, identification, authentication, and authorization parts of the proposed solution be integrated with NCDOT Active Directory.

If Active Directory integration is not specifically required in the RFP, the solution shall integrate with the North Carolina Identity Management Solution (NCID) [using SAML v2 – NCID SAML v2 Authentication](#). Refer to the NCID website for more information: <https://it.nc.gov/ncid-help>

The following requirements for authentication and authorization shall be met:

1. A single user ID shall control all functions for a specific user without requiring multiple logins.
2. The proposed solution shall allow for role-based access to functions, as defined by NCDOT.
3. The proposed solution shall authenticate users in a DMZ prior to allowing access to the application or business logic tier.

I. Systems Administration

If the proposed solution is a NCDOT hosted “on premise” solution the following apply:

1. The proposed solution shall be hosted and managed by NCDOT staff via software releases provided by the Vendor.
2. All system administrative functions shall be available through a graphical user interface.
3. The proposed solution shall provide the capability to generate ad-hoc audit reports of all system administration activities.
4. Vendor shall provide sufficient documentation to install, maintain, and test new releases of vendor software for any release component to enable NCDOT to install, test, and maintain the release with minimal Vendor support.
5. Errors detected at any validation point shall be reported in such a way that a NCDOT staff will know what corrective action must be taken to resolve the error.
6. Rerun and/or restart capability shall be clearly defined and integrated in the proposed solution such that the NCDOT staff can resume production operation for all components.
7. Any enhancements to the proposed solution architecture shall be submitted and approved by the NCDOT Architecture Team (and may be subject to approval at the statewide level) with enough advance notice to avoid disruption to the operating environment and solution users.
8. All changes to the deployed solution shall be approved prior to implementation by the NCDOT change management process.

J. Change Management

The proposed solution and the vendor shall use and follow all applicable State and NCDOT change management procedures and processes.

K. Maintenance Windows

The awarded Vendor shall utilize NCDOT’s standard maintenance windows of Sundays between 4am and 12pm and Thursdays between 4am and 7am for change and maintenance implementation.

L. Solution Documentation

The vendor shall provide documentation for the proposed solution as follows:

- System Architecture documentation for all components and interfaces
- Network Architecture documentation for all components and interfaces
- Solution logical process flow documentation

If the proposed solution is a NCDOT hosted “on premise” solution the following apply:

- Solution installation documentation for all required components including client setup
- Operational Support documentation (including but not limited to)
 - Diagnostic troubleshooting
 - Service Desk procedures and processes
 - Solution Backup and Recovery steps and processes
 - Update / upgrade steps and processes

M. Data and System Security

The proposed solution must meet minimum security standards and guidelines as defined in the North Carolina Statewide Information Security Manual found at: <http://it.nc.gov/statewide-resources/policies>

The proposed solution must comply with all applicable laws and regulations and take appropriate measures to protect NCDOT data that may be contained within the solution.

The proposed solution must handle the State's information, data and documents in a manner that will protect the information, data and documents from unauthorized or accidental disclosure, modification or loss.

The proposed solution must provide for secure communications that are encrypted to provide confidentiality based on FIPS 140-2 approved encryption Transport Layer Security (TLS) communication protocols.

The proposed solution must be capable of classifying, protecting, and controlling NCDOT data and the systems they reside on via role-based access control entitlements.

The proposed solution must insure that NCDOT data will not be hosted outside of US legal borders.

The proposed solution shall be compatible with NCDOT's host-based, intrusion detection software and all hardware shall be appropriately sized to support this software.

N. Auditing

The proposed solution shall maintain auditable logs of all user activities performed and shall be compatible with syslog or agent transfer to NCDOT's IBM QRadar SIEM system for collection and analysis.

Logs shall include the following at a minimum:

- All actions taken by any individual with administrative privileges
- Date and time an auditable event occurs
- Access to all Audit trails
- Invalid or valid logical access attempts
- Use of identification and user mechanisms
- Initialization of audit logs
- Creation and deletion of system-level objects
- All log sources shall be synchronized with an NCDOT approved Network Time Protocol (NTP) source.
- The identity and role of the actor performing the activity. If an identity can be assigned multiple roles, or multiple roles can authorize the same activity, this would mean the role used to authorize the activity in this case.
- The outcome (success or failure) of the activity.

O. Electronic Payments

The proposed solution and all components provided by the Vendor or by any service provider(s) that may be processing, transmitting, or storing payment data, shall be in compliance with all applicable payment industry standards. The standards include those issued by the National Automated Clearing House Association (NACHA), by the Payment Card Industry Security Standards Council, and by the various merchant card brands.

Reference links include:

<http://www.nacha.org/c/achrules.cfm>

<https://www.pcisecuritystandards.org>

Vendor response shall address how the Agency's existing enterprise services will be used in processing electronic payments. The State's current electronic payment system is described at the following link:

<http://www.osc.nc.gov/SECP/index.html>.

P. Accessibility

The State requires that websites and applications be accessible for people with disabilities. Any public-facing applications and/or interfaces produced for NCDOT shall comply with:

- Section 508 of the Rehabilitation Act (29 U.S.C. 794d).
- Web Content Accessibility Guidelines (WCAG) 2.0.

Q. Platform Architecture Standards: Mobile Devices¹

COMPONENT	ENVIRONMENT
Platform	Windows, iOS and Android
Software Compatibility	ESRI Map Services, feature Services, data Services, image Services, Geoprocessing Services
Web Service - Data Formats	JSON
Web Service – Data Exchange	REST
Application Development Frameworks	Jquery Mobile, DOJO
Content Rendering	Cascading Style Sheets (CSS3)
Client Side Scripting	AJAX/JQuery/JavaScript (ECMAScript v5)
Markup	HTML5, XML
Authentication	NCID Active Directory
Connectivity	Verizon Wireless Cellular data 3G, 4G Wi-Fi (WPA2 Enterprise Security)

¹ Vendor's mobile solution offerings must deliver functionality outlined within this RFP, including adherence to GIS standards.